L'AVOCAT A-T-IL AUSSI LE DROIT D'ÊTRE DANS LES NUAGES?

YANIV BENHAMOU
avocat, chargé de cours à l'Université de Genève

FRÉDÉRIC ERARD
assistant doctorant à l'Institut de droit de la santé de l'Université de Neuchâtel, avocat

DANIEL KRAUS[1]
professeur ordinaire à l'Université de Neuchâtel, directeur du Pôle de Propriété intellectuelle et de l'innovation [PI][2], avocat

Mots-clés: gestion des données d'une étude, informatique, secret professionnel, diligence, externalisation des données

La présente contribution se base sur les présentations faites par les auteurs lors de la journée des avocats du 15 juin 2018. Elle s'inscrit dans le prolongement de différents articles rédigés par des confrères sur la question du Cloud et examine en particulier l'influence du devoir de diligence dans ce contexte. Elle aborde en outre la question de la protection des données et des devoirs de confidentialité en vue de tracer des pistes entre l'ancien monde analogique et le nouveau monde numérique, ce dernier offrant à la fois des opportunités et des défis aux avocats et leur clientèle.

I. Introduction

À l'heure des legaltech, la profession d'avocat est sous pression. De plus en plus de prestataires IT de services juridiques arrivent sur le marché et proposent différentes prestations (p. ex. mises en contact entre l'avocat et le client, consultations, résolutions de litiges en ligne)[2]. Au vu de l'évolution du métier, d'aucuns prévoient la fin de la profession[3]. Or, après le monde de la musique, des taxis, de l'hôtellerie et même des services d'assurances et de banques, le monde des avocats est probablement l'un des derniers à avoir amorcé sa transformation numérique.

La discussion autour de l'utilisation de l'informatique en nuage (Cloud) par les avocats ne présente qu'un aspect de cette transformation numérique[4]. Il en constitue vraisemblablement le plus récent. Car les moins jeunes se rappelleront de la résistance qu'ont opposée les avocats à l'utilisation de l'internet, puis du courrier électronique, dans l'exercice de leur profession. Or, comme le fax dès la fin des années 1980, l'utilisation de l'internet pour des recherches et de l'e-mail pour la communication avec la clientèle est devenue chose courante, alors même que ces technologies sont loin d'être infaillibles du point de vue de la confidentialité[5]. Même s'il est vrai que l'utilisation de l'informatique en nuage présente de nombreux avantages, comme l'utilisation du fax (en son temps), du mail, du téléphone portable et de l'internet en général, il convient d'examiner le cadre juridique dans lequel le Cloud peut être utilisé par les avocats. La question a été principalement analysée sous l'angle pénal (risques liés à la violation

1 Les auteurs remercient vivement Mes Emilie Jacot-Guillarmod, Wolfgang Straub et David Vasella pour leurs précieux commentaires.

2 Pour un aperçu des différentes prestations IT dans le domaine juridique (p. ex. Cloud, Legaltech, Legal Marketplaces) et des enjeux juridiques, *cf.* TANO BARTH, Utilisation des nouvelles technologies: devoir de diligence de l'avocat, Jusletter du 3. 9. 2018.

3 RICHARD SUSSKIND, The End of Lawyers, 2010.

4 L'utilisation d'une solution Cloud peut se définir comme l'accès à distance à des composantes IT, soit à des infrastructures IT *(hardware)* et/ou à des fonctionnalités IT *(software).* Suivant les services fournis par le Cloud Provider, on parle de SaaS *(Software-as-a-service)* lorsque l'avocat n'utilise que certaines fonctionnalités IT *(softwares),* de IaaS *(Infrastructure-as-a-service)* lorsque l'avocat utilise les infrastructures du Cloud Provider et de XaaS *(Everything as a service)* lorsque l'avocat utilise les deux composantes IT, infrastructures et fonctionnalités. CHAPPUIS/ALBERINI, Secret professionnel de l'avocat et solutions cloud, Revue de l'avocat 8/2017, p. 337, 338.

5 Le fax constitue même une porte d'entrée privilégiée pour accéder à des données personnelles, *cf.* Les fax menacent la sécurité des entreprises, Le Temps, 20. 8. 2018, en ligne: www.letemps.ch/economie/fax-menacent-securite-entreprises (consulté le 8. 1. 2019). L'article fait référence à une étude en cybersécurité dont les résultats peuvent être consultés ici: <https://research.checkpoint.com/sending-fax-back-to-the-dark-ages> (consulté le 8. 1. 2019).

du secret professionnel protégé par l'article 321 CP), en particulier WOHLERS qualifiant le Cloud Provider comme un tiers (non comme un auxiliaire) et considérant que le client doit consentir de manière explicite ou par acte concluant à l'usage du Cloud par son avocat et CHAPPUIS/ALBERINI considérant le Cloud Provider comme un auxiliaire couvert lui aussi par le secret professionnel et que le consentement du client n'est ainsi pas nécessaire[6].

Nous proposons d'analyser la question non seulement sous l'angle de l'épée de Damoclès pénale, mais aussi sous celui des obligations que l'avocat doit respecter afin de servir au mieux les intérêts légitimes de ses clients. La question doit donc être envisagée sous trois angles. Premièrement, sous l'angle du devoir diligence contractuel (art. 398 al. 2 CO) et professionnel (art. 12 let. a LLCA). Sous cet angle, la question est de savoir quel avocat est le plus diligent: celui qui utilise le Cloud de manière précautionneuse ou celui qui y renonce (1). Deuxièmement, sous l'angle de la protection des données (2). Et enfin seulement, sous l'angle pénal de l'obligation de respecter le secret professionnel (art. 321 CP) (3).

II. Le devoir de diligence contractuel (art. 398 al. 2 CO) et professionnel (art. 12 let. a LLCA)

1. Responsabilité de l'avocat envers le mandant

L'avocat a un devoir de diligence contractuel et professionnel envers son mandant; il est responsable de la bonne et fidèle exécution du mandat envers le mandant (art. 398 al. 2 CO et art. 12 let. a LLCA). Lorsqu'ils visent le mandant[7], l'art. 398 al. 2 CO et l'art. 12 let. a LLCA ont une portée pratiquement similaire et doivent donc être interprétés selon les mêmes principes[8]. Toutefois, seules les violations du devoir de diligence d'une *certaine gravité,* intentionnelles ou gravement négligentes sont passibles de sanctions disciplinaires au sens de l'art. 17 LLCA[9]. Toute violation du droit contractuel n'est donc pas forcément sanctionnable sur le plan disciplinaire[10].

La diligence requise ne peut pas être définie de manière abstraite, mais dépend de la nature des activités et de l'ensemble des circonstances concrètes[11]. Le mandataire doit agir *«comme le ferait une personne raisonnable et diligente dans des circonstances semblables»*[12]. Sous l'angle des *mesures d'organisation interne,* l'obligation de diligence impose à l'avocat de se doter d'une *structure minimale de travail* lui permettant d'exercer ses activités dans le respect des obligations qui lui sont imposées[13], dont une *infrastructure informatique permettant d'assurer* la sécurité des données[14]. À cet égard, toute une série de précautions doivent être adoptées, notamment: choisir un système informatique cohérent, prévoir un système de duplication des données, assurer une maintenance suffisante, effectuer des sauvegardes journalières, se protéger contre le phénomène d'obsolescence, se doter de systèmes de sécurité fiables contre les attaques informatiques[15]. L'avocat qui perdrait des informations enregistrées sur son seul ordinateur personnel suite à une panne faillirait à son devoir de diligence[16]. En raison de la nature des dossiers traités et des attentes des clients, le niveau de protection des installations exigible peut toutefois *varier selon le type d'études et la nature des dossiers* traités, tout comme ce serait le cas avec des dossiers physiques[17].

Le Cloud comporte non seulement des avantages pour l'avocat (p. ex. réduction des coûts, simplicité d'utilisation), mais peut aussi favoriser la protection des données client. C'est particulièrement le cas pour les clients des études dont les ressources sont limitées. Pour autant qu'elles soient correctement concrétisées, les solutions Cloud offrent aujourd'hui *une sécurité renforcée* des données par rapport aux solutions *in house* et traditionnelles (p. ex. postes informatiques individuels, enregistrement sur un support externe susceptible d'être volé ou détruit, transport risqué d'un support de données vers un coffre, serveurs installés dans des pièces inadéquates, logiciels obsolètes exposant à des risques[18]). Sans négliger les risques en présence, on peut *se demander si le recours au Cloud n'est pas aujourd'hui dicté par le devoir de diligence* de l'avocat dans l'hypothèse où ce dernier ne serait pas en mesure d'équiper son étude d'un système informatique *in house* suffisamment efficace, constamment à jour et sécurisé.

Si le mandataire est un spécialiste, son *devoir de diligence se mesure à l'aune du degré de spécialisation.* Dans cette situation, les *règles de l'art* généralement reconnues

---

6 WOLFGANG WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis, 2016, p. 55; CHAPPUIS/ALBERINI, (n. 4), p. 340; *cf.* aussi récemment TANO BARTH, (n. 2), N 13, qui examine la question principalement sous l'angle du devoir de diligence de l'avocat et considère que l'avocat doit pouvoir recourir au Cloud même depuis l'étranger, à l'exception des cas où des éléments du dossier et les pratiques de l'État concerné laissent penser qu'il existe un risque concret que les autorités de cet État puissent tenter d'accéder ou exiger l'accès aux données clients.

7 Le devoir de diligence contractuel est essentiellement érigé dans l'intérêt du mandant, tandis que le devoir de diligence professionnel a une portée plus large en tant que le cercle de bénéficiaires s'étend à d'autres bénéficiaires que le mandant, tels que les autorités, les confrères, les parties adverses et les témoins. Cf. BENOÎT CHAPPUIS, La profession d'avocat, Tome I, 2e éd. 2016–2017, p. 52.

8 BENOÎT CHAPPUIS, (n. 7), p. 53.

9 WALTER FELLMANN, in Kommentar zum Anwaltsgesetz, 2011, no 26 ad art. 12 BGFA.

10 FRANÇOIS BOHNET, Droit des professions judiciaires. Avocat. Notaire. Juge, 3e éd. 2014, p. 35.

11 TERCIER/BIERI/CARRON, Les contrats spéciaux, 5e éd. 2016, N 4436; FRANZ WERRO, in Commentaire romand, Code des Obligations I, 2e éd. 2012, no 14 ad art. 398 CO.

12 FRANZ WERRO, (n. 11), no 14 ad art. 398 CO.

13 BENOÎT CHAPPUIS, La profession d'avocat, tome II, 2e éd. 2017, p. 8. CHAPPUIS précise que s'il s'agit là de l'opinion majoritaire, certains auteurs déduisent l'obligation d'organisation des conditions d'inscription au registre cantonal.

14 WOLFGANG STRAUB, Qu'apportent l'informatique et les nouvelles technologies dans les études d'avocats (1re partie), Revue de l'avocat 11-12/2012, p. 518.

15 VINCENT JEANNERET, Le «risk management» dans une étude d'avocats, in Défis de l'avocat au XXIe siècle, Mélanges en l'honneur de Madame le Bâtonnier Dominique Burger, 2008, p. 397, 400–403.

16 CHAPPUIS/ALBERINI, (n. 4), p. 340.

17 WOLFGANG STRAUB, (n. 14), p. 518.

18 Sur ces risques: CHAPPUIS/ALBERINI, (n. 4), p. 340, 342.

et les *règles déontologiques* peuvent servir de référence pour déterminer le devoir de diligence[19]. La plupart des *règles professionnelles et déontologiques sont toutefois muettes* sur l'externalisation du traitement de données. Le *Code de la FSA* se contente d'affirmer, de manière similaire à la LLCA, que l'avocat impose le *respect du secret professionnel* à ses collaborateurs, employés et auxiliaires (art. 15 al. 3 Code FSA) et n'apporte pas de précision quant au recours au Cloud par l'avocat. On peut se demander si la FSA ou les barreaux cantonaux pourraient jouer un rôle plus actif et préciser les conditions pour recourir au Cloud, à l'image des Circulaires FINMA dans le secteur bancaire[20]. Comme indiqué par CHAPPUIS/ALBERINI, *«une telle approche risquerait de faire peser une charge réglementaire excessive sur les avocats, dont les structures et la manière de pratiquer diffèrent substantiellement de celles des banques».* Alternativement, il serait envisageable d'édicter des recommandations de bonnes pratiques, de proposer des contrats-modèles avec les prestataires IT et/ou d'aider à identifier les prestataires IT réputés offrir un cadre suffisant en matière de sécurité des données[21]. Par exemple, le Conseil des barreaux européens *(CCBE) a émis des lignes directrices* sur le recours à l'informatique en nuage par les avocats[22]. Celles-ci mettent en lumière de manière précise toute une série de points auxquels les avocats doivent porter une attention particulière lorsqu'ils recourent aux services d'un prestataire Cloud, y compris la possibilité pour les avocats européens de recourir à des fournisseurs établis dans l'EEE et le conseil d'éviter *«une juridiction dont l'étendue de la législation l'oblige à divulguer les données d'avocats européens conservées sur un serveur en nuage, comme ce pourrait être le cas, à des autorités nationales extérieures à l'Union européenne»*[23]. Si ces lignes directrices s'adressent en premier lieu aux barreaux membres du CCBE, elles constituent une source d'inspiration particulièrement utile pour la construction des relations entre avocats et prestataires Cloud.

En l'absence de dispositions légales et de règles professionnelles précises, déterminer si le respect du devoir de diligence de l'avocat impose de recourir à une solution Cloud est une question à laquelle il est difficile de répondre dans l'abstrait. À notre sens, *cette solution pourrait progressivement s'imposer lorsque l'avocat n'est pas en mesure de se doter d'une infrastructure in house* suffisamment sécurisée. L'avocat qui se passe d'une telle solution et qui subit des pertes ou des vols de données évitables par le recours au Cloud faillirait probablement à son devoir de diligence. Cette conclusion est amenée à s'ancrer plus fermement dans le temps, au fur et à mesure des avancées technologiques à venir.

2. Responsabilité de l'avocat pour les actes du Cloud Provider

La responsabilité de l'avocat pour les actes du Cloud Provider dépendra de la qualification de ce dernier.

Si le Cloud Provider est *qualifié d'auxiliaire simple* au sens de l'art. 101 CO, l'avocat répondra des actes du Cloud Provider comme des siens, même s'il n'a commis aucune faute quant au choix, instructions et surveillance du Cloud Provider[24]. L'auxiliaire au sens de l'art. 101 CO est compris de manière large comme les personnes commettant des actes dans l'accomplissement de l'obligation de l'avocat (ce qui devrait inclure le personnel de nettoyage, contrairement à la notion d'auxiliaire au sens de l'art. 321 CP)[25]. L'avocat devra alors *répondre du comportement du Cloud Provider* comme s'il s'agissait du sien propre. Il peut toutefois s'exonérer en prouvant qu'aucune faute ne lui serait imputable s'il avait agi personnellement comme l'a fait le Cloud Provider[26]. Cela dit, lorsque la prestation du tiers revêt une composante technique particulière (à l'image des prestations Cloud), la référence aux compétences personnelles de l'avocat se révèle inadéquate. Dans ce cas, il convient de prendre pour référence les *«qualifications objectivement nécessaires à la bonne exécution de la prestation promise, en tenant compte des règles de l'art, des usages professionnels et de l'état de la technologie, indépendamment des qualités personnelles du débiteur ou de*

19 FRANZ WERRO, (n. 11), nº 14 ad art. 398 CO.

20 *Cf.* en particulier la Circulaire FINMA 2018/7 Outsourcing – banques et assureurs, n. 40.

21 Des efforts notables et des discussions sont à mentionner ici, p. ex. à l'échelon cantonal en matière de protection des données ODAGE (*cf.* document explicatif «De l'actuelle loi sur la protection des données [LPD] au projet de révision du 15. 9. 2017 [P-LPD] en passant par le nouveau règlement européen sur la protection des données du 27. 4. 2016 [RGPD]») et avec le travail de commissions spécialisées, telles que la Commission Innovation et Modernisation du Barreau de Genève (CIMBAR); à l'échelon national, avec des discussions en cours au sein de la FSA sur l'utilisation de prestataires IT et les travaux de la commission FSA «Digitalisierung».

22 CCBE, Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, 7. 9. 2012, en ligne: <www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20110909_CCBE_Response_on_Cloud_Computing.pdf> (consulté le 8. 1. 2019).

23 CCBE, Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, 7. 9. 2012, p. 6. On peut également mentionner dans le domaine médicial, le Guide pratique «Bases juridiques pour le quotidien du médecin» de l'Académie Suisse des Sciences Médicales (ASSM) et de la Fédération des médecins suisses (FMH), 2e éd., 2013, recommandant pour la protection des données et en particulier pour l'échange électronique des données (chap. 7.2): *«Il n'est permis d'échanger des données de patients […] que par courrier électronique protégé: les courriels doivent être cryptés. À cet égard, le réseau HIN ('Health Info Net') et la carte CPS de la FMH permettent un cryptage sûr».* Si l'on peut douter d'une telle recommandation quant à la charge (aussi financière) que de tels systèmes font peser sur les médecins, alors que ces derniers pourraient obtenir le consentement des patients à l'échange de données non cryptées, et relever l'incertitude juridique quant au caractère obligatoire d'une telle recommandation, le guide a au moins le mérite de traiter cette question et de tenter d'apporter des réponses.

24 LUC THÉVENOZ, in Commentaire romand, Code des Obligations I, 2e éd. 2012, nº 25 ad art. 101 CO.

25 BOHNET/MARTENET, Droit de la profession d'avocat, 2009, N 3107; WALTER FELLMANN, Anwaltsrecht, 2e éd. 2017, N 1563; SURY/GOGNIAT, Umzug einer Kanzlei in die Cloud, Revue de l'avocat 5/2015, p. 201, 203.

26 LUC THÉVENOZ, (n. 24), nº 26 ad art. 101 CO; BENOÎT CHAPPUIS, (n. 13), p. 185.

ses organes»[27]. Cependant, cette preuve libératoire est difficile à apporter et échoue souvent[28]. L'avocat aura donc tout intérêt à choisir consciencieusement le Cloud Provider et à s'assurer que la sous-traitance des données s'effectuera en conformité avec la loi et ses obligations à l'égard de ses clients[29].

Si le Cloud Provider est *qualifié de substitut autorisé* au sens de l'art. 398 al. 3 CO et 399 al. 2 CO, l'avocat ne répondra des actes du Cloud Provider que sous l'angle des *trois curae* (choix, instruction et surveillance)[30]. La qualification de substitut autorisé (plutôt que d'auxiliaire) dépend des critères de distinction suivants: absence d'intérêt économique de l'avocat, participation principale du Cloud Provider à l'exécution, expertise particulière du Cloud Provider, intérêt du client à la substitution ainsi que l'indépendance économique et pratique du Cloud Provider par rapport au mandataire[31]. Sur cette base, le Cloud Provider aura tendance à être qualifié de susbtitut autorisé: l'avocat recourt généralement au Cloud, non seulement dans son propre intérêt économique (p. ex. réduction des coûts, simplicité d'utilisation) et avec une participation plutôt accessoire du Provider à l'exécution du mandat (p. ex. stockage ou facturation) mais aussi dans l'intérêt du client (sécurité accrue des données avec des prestataires indépendants à forte expertise). La responsabilité de l'avocat aura ainsi tendance à être limitée aux *trois curae,* étant rappelé que ce seront principalement les *curae* de choix et d'instruction qui seront déterminantes, faute de compétences techniques de l'avocat pour assurer la *cura* de surveillance du Cloud Provider.

III. La protection des données

1. *1. Données cryptées ou pseudonymisées avant l'envoi dans le nuage*

Le recours au Cloud par l'avocat devra être conforme au droit de la protection des données. Relevons d'emblée que la question de *protection des données* ne se posera *pas* si le Cloud Provider n'a *pas accès au contenu des données,* par exemple parce qu'elles lui sont envoyées sous forme *cryptée* ou *pseudonymisée* et que la clé de cryptage, respectivement le tableau de correspondance, reste sous le contrôle de l'avocat[32]. La question de protection des données ne se posera que si le Cloud Provider a accès au contenu des données, par exemple parce que les données lui sont envoyées en clair ou parce qu'il a accès à la clé de cryptage ou tableau de correspondance. Il serait ainsi intéressant, voire préférable de recourir à ce type de solutions pour éviter les considérations suivantes.

2. *Sous-traitance des données aux conditions de l'art. 10a LPD*

Lorsque le Cloud Provider a accès aux données, le traitement des données personnelles par le Cloud Provider sera possible aux conditions de l'art. 10*a* LPD.

– Le traitement devra être soumis à un *contrat garantissant la protection des données* (art. 10*a* al. 1 et al. 2 LPD). Vu la variété des prestations envisageables (SaaS, PaaS, IaaS), la qualification du contrat ne peut se faire abstraitement mais on relèvera que le dénominateur commun est la fourniture de services liés aux technologies du Cloud Provider et qu'il s'agira d'un contrat nommé (vente, entreprise, mandat, bail, société simple) ou innommé (mixte ou *sui generis*)[33]. Le contrat devra prévoir en particulier les mesures techniques et organisationnelles permettant de garantir la sécurité des données (art. 7 LPD, 8 OLPD)[34], l'objet et la durée du traitement, la nature et la finalité du traitement et, pour les services soumis au RGPD, l'obligation d'obtenir l'autorisation préalable avant toute sous-traitance de 2e degré. Il faudra par ailleurs prévoir que les employés du Cloud Provider ne devront pas avoir accès aux données personnelles, sauf cas exceptionnels limités à certains employés *(need-to-know basis)* et qu'ils seront soumis à des règles strictes de confidentialité.

---

27 LUC THÉVENOZ, (n. 24), no 30 ad art. 101 CO.

28 LUC THÉVENOZ, (n. 24), no 26 ad art. 101 CO; BENOÎT CHAPPUIS, (n. 13), p. 185.

29 Pour une série d'exigences et de précautions à prendre en compte lors du recours à un prestataire Cloud par un avocat, voir notamment: SÉBASTIEN FANTI, Cloud computing: opportunités et risques pour les avocats, Revue de l'avocat 2/2013, p. 74, 76; CHAPPUIS/ALBERINI, (n. 4), p. 341; CCBE, Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, 7. 9. 2012, en particulier p. 8–9; en ligne: <www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20110909_CCBE_Response_on_Cloud_Computing.pdf> (consulté le 8. 1. 2019).

30 CHAPPUIS/ALBERINI, (n. 4), p. 341, qui recourent à la triple *curae* et expliquent que seules les curae de choix et d'instruction seront déterminantes, puisque l'avocat pourra difficilement surveiller le Cloud Provider pour des prestations hautement techniques, faute de compétences spécifiques de l'avocat en matière technique.

31 FRANZ WERRO, (n. 11), no 5 ad art. 398 CO.

32 Le PFPDT avait émis une position plus stricte, dans le cadre d'une consultation de la FINMA en 2013. Il considérait qu'il fallait se placer tant du point de vue de l'expéditeur de la donnée (p. ex. l'avocat expéditeur des données au Cloud Provider) que du destinataire de la donnée (p. ex. Cloud Provider recevant les informations de l'avocat). L'information serait qualifiée de donnée personnelle dès que l'une des deux parties aurait des moyens de ré-identification (approche dite alternative). Ainsi, les informations communiquées au Cloud Provider seraient qualifiées de données personnelles, même si l'avocat est le seul à accéder aux données personnelles, p. ex. avec la clé de cryptage des données anonymisées, ou le tableau de correspondance des données pseudonymisées. Externalisation à l'étranger de données bancaires pseudonymisées, 2013. Cette position semble désormais dépassée suite à l'arrêt du TF confirmant que les données pseudonymisées échappent à la LPD si la pseudonymisation empêche effectivement l'identification de la personne concernée du point de vue du destinataire des informations. Arrêt du TF 4A_365/2017 du 26. 2. 2018. *Cf.* aussi privatim, Prise de position, Privatisation et secret médical, 17. 5. 2017. Relevons également que l'écoulement du temps joue un rôle déterminant quant à l'efficacité des techniques de cryptage et de pseudonymisation (qui pourront être plus aisément «contournées» au fur et à mesure de l'écoulement du temps et de l'essor des technologies) et qu'il faudra mettre à jour continuellement les techniques de cryptage ou de pseudonymisation (p. ex. migrer les données vers de nouvelles clés et effacer les anciennes données).

33 *Cf.* JACCARD/ROBERT, Les contrats informatiques, in La pratique contractuelle: actualité et perspectives. Symposium en droit des contrats, 2009, p. 95 ss; NAYDA COCHET-SEBASTIAN, Les contrats informatiques, ECS 8/2011, p. 611.

34 Les mesures techniques et organisationnelles sont souvent prévues dans une annexe au contrat de prestation, ou par renvoi à des normes standards (p. ex. ISO 27001, 27002) dont le prestataire garantit la certification.

- Le Cloud Provider ne pourra par ailleurs effectuer que les *traitements que le mandant serait en droit d'effectuer lui-même* (art. 10*a* al. 2 let. a LPD) et pourra le cas échéant faire valoir les mêmes motifs justificatifs que le mandant (art. 10*a* al. 3 LPD). L'avocat traite de nombreuses données, notamment celles de ses clients et de tiers.[35] Leur traitement doit être conforme aux principes généraux (en particulier finalité, reconnaissabilité et sécurité des données au sens des art. 4 ss LPD). Pour les données clients, le traitement sera par ailleurs généralement justifié par le consentement du client, ou au moins reconnaissable du client, dans le cadre de l'exécution du mandat. Pour les données de tiers, le traitement pourra être justifié par un intérêt prépondérant privé de l'avocat et du client à traiter des données de tiers (art. 13 al. 1 LPD).
- *«Aucune obligation légale ou contractuelle de garder le secret»* n'interdira le recours au Cloud Provider puisque le Cloud Provider est qualifié d'auxiliaire au sens de l'art. 321 CP (art. 10*a* al. 1 let. b LPD). Dans l'attente de règles ou de décisions claires quant à la qualification du Cloud Provider comme auxiliaire au sens de l'art. 321 CP, l'approche prudente consiste à considérer le Cloud Provider comme un tiers (et non comme un auxiliaire) et à privilégier le consentement préalable du client. Le consentement doit être libre et éclairé (en particulier le but du traitement doit être compréhensible tout comme le type de données collectées) (art. 4 al. 5 LPD)[36]. Il n'est soumis à aucune exigence de forme (art. 11 CO), il peut être exprès, tacite ou donné par actes concluants[37]. S'agissant de données couvertes par le secret de l'avocat, il est risqué d'admettre un consentement tacite vu la nature confidentielle des données[38]. En l'absence de consentement exprès ou tacite, on pourrait éventuellement plaider qu'il existe un motif justificatif au traitement (art. 12 al. 2 let. b LPD), puisqu'un tel *«traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie»* (art. 13 al. 2 let. a LPD).

Sous l'angle du *RGPD* (et par anticipation du P-LPD), la communication des données personnelles devra être en outre conforme aux *exigences en matière de transparence et d'information* à fournir, en particulier le client devra être informé de l'identité du Cloud Provider (destinataires) ou au moins de l'existence de prestataires informatiques (catégories de destinataires) (art. 13 al. 1 let. e RGPD; art. 17 al. 2 let. c P-LPD)[39]. Ces informations devront être fournies au moment de la collecte des données client, ce qui suppose leur insertion dans des conditions générales (p. ex. politique de confidentialité affichée sur le site web de l'étude) et/ou de la lettre d'engagement de l'avocat.

3. Sous-traitance des données à l'étranger (art. 6 LPD)

Enfin, le recours à des Cloud Providers étrangers supposera de respecter les règles en matière de transfert à l'étranger (art. 6 LPD), étant précisé que cette problématique existe déjà lorsque l'avocat utilise des services de *legal tech*[40], voire consulte ses e-mails depuis l'étranger[41] et que cette distinction entre prestataires suisses et étrangers devient de plus en plus artificielle en cas de prestataire partie à un groupe étranger dont la société mère sise à l'étranger a un pouvoir de fait sur les données contrôlées par la société suisse. Une telle communication sera *possible* dans un *pays à niveau de protection adéquat ou,* en l'absence d'un niveau de protection adéquat, à la condition de mettre en place des *garanties contractuelles* avec le prestataire. Dans tous les cas, le client devra pouvoir reconnaître que ses données sont transférées à l'étranger (principe de reconnaissabilité, art. 4 al. 1 LPD) et, en cas de

35 Une question qui n'a à notre avis pas encore été tranchée mais déterminante puisqu'elle définirait les obligations liées à la protection des données entre l'avocat et le client (notamment l'obligation de conclure un data processing agreement entre l'avocat et le client) est celle de savoir si l'avocat peut être qualifié de sous-traitant (processor). Nous sommes d'avis que ce n'est pas le cas, en particulier vu l'indépendance de l'avocat et la marge de manœuvre dont il dispose pour le traitement des données clients. Cette question dépasse toutefois la présente contribution.

36 La personne concernée doit recevoir en termes clairs, intelligibles et aussi complets que possible les informations relatives au traitement. *Cf.* PHILIPPE MEIER, Protection des données, 2011, N 849, expliquant que cette notion de «consentement libre et éclairé» est directement importée de la jurisprudence en droit médical.

37 PHILIPPE MEIER, (n. 35), N 874.

38 Par comparaison, en droit bancaire, il est controversé de savoir si le consentement implicite est possible ou si le consentement doit être toujours exprès. Pour les services soumis au RGPD (et par anticipation avec la révision de la LPD, selon le projet actuel P-LPD), l'avocat devra par ailleurs tenir compte des nouvelles exigences en matière de consentement qui supposent un *«acte positif clair»* (*cf.* art. 4 ch. 11 RGPD et cons. 32: *«Le consentement devrait être donné par un acte positif clair […] Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité»*) et pourraient exclure le recours au consentement implicite. À propos du champ d'application «extra-territorial» du RGPD au sens de l'art. 3 § 2 RGPD, cf. BENHAMOU/JACOT-GUILLARMOD, GDPR on the Swiss Territory, Jusletter IT du 24. 5. 2018; cf. lignes directrices du EDPB sur le champ d'application du RGPD, rendues publiques le 23. 11. 2018 et soumises à consultation publique jusqu'au 18. 1. 2019.

39 Message P-LPD, FF 2017 6565, 6669: *«les sous-traitants font partie des destinataires au sens de la disposition. Si le responsable du traitement ne souhaite pas révéler l'identité des destinataires, il peut se contenter d'indiquer leur catégorie.»*

40 Nombre de ces services *legal tech* supposent en effet une externalisation des données à l'étranger (non cryptées ou non pseudonymisées). Pour un aperçu général des legal tech et des problématiques juridiques qu'elles soulèvent, *cf.* TANO BARTH, (n. 2), p. 2 ss.

41 Selon une interprétation restrictive (littérale), la consultation d'e-mails depuis l'étranger constitue un cas de communication (passive) hors de Suisse, en particulier puisque l'avocat n'a en principe pas eu auparavant connaissance des données contenues dans l'e-mail qui lui est envoyé. Cf. SÉBASTIEN FANTI, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), in Internet au travail, 2014, p. 185. Selon une interprétation large (téléologique), il n'y aurait toutefois pas de communication transfrontière, puisqu'une telle communication suppose d'étendre le cercle de destinataires à l'étranger (personnes accédant aux données depuis l'étranger). Or, la simple consultation d'e-mails depuis l'étranger n'étend pas le cercle de personnes accédant aux données de l'avocat. Cf. JEAN-PHILIPPE WALTER, Communication des données personnelles à l'étranger, in Die Revision des Datenschutzgesetzes, 2009, p. 119. Voir également PHILIPPE MEIER, (n. 35), N 1272, tout en notant ici que l'auteur se prononce dans le contexte de déplacements temporaires et épisodiques à l'étranger et non du télétravail. Voir également DAVID ROSENTHAL, in Handkommentar zum Datenschutzgesetz, 2008, nº 6 ad art. 6 DSG.

transfert de pays à niveau de protection non équivalent, être informé des garanties appropriées et des pays dans lesquels les données sont envoyées[42]. En l'absence de consentement et d'information spécifique, on pourrait éventuellement plaider qu'il existe un motif justificatif au traitement (art. 12 al. 2 let. b et 13 al. 2 let. a LPD, traitement «nécessaire à l'exécution d'un contrat», voire même art 13. al. 1 LPD, «intérêt prépondérant privé» de l'avocat).

Sur cette base, en l'absence de dispositions légales ou de règles professionnelles précises[43], nous ne voyons pas d'obstacle à recourir à un Cloud Provider établi à l'étranger, pour autant que les conditions de la LPD soient respectées (pays à niveau de protection adéquat ou moyennant garanties contractuelles) ainsi que le secret professionnel au sens de l'art. 321 CP et le devoir de diligence contractuel et professionnel. Puisque ces considérations concernent la protection des données uniquement et sont sans préjudice des principes en matière pénale du respect du secret professionnel et du devoir de diligence:

- il sera *prudent de requérir le consentement exprès* du client vu la nature confidentielle des données et les exigences élevées en matière de consentement, et de ne pas se contenter du consentement tacite, ou d'éventuels motifs justificatifs, via l'insertion d'informations détaillées dans les conditions générales et/ou la lettre d'engagement[44];
- certaines juridictions pourront être par ailleurs réputées plus risquées que d'autres, soit celles dont la législation oblige l'avocat à divulguer les données hébergées sur un Cloud sans garanties procédurales visant à protéger le secret professionnel («risque pays»). Vu ce risque pays et le devoir de diligence exposé, l'avocat devrait *privilégier des Cloud Providers établis en Suisse,* ou au moins dans l'UE, dont les législations prévoient généralement un niveau de protection élevé des données et des garanties en matière de secret professionnel similaires au droit suisse[45].

IV. Le droit pénal

1. Le Cloud Provider en tant qu'auxiliaire de l'avocat

Sous l'angle pénal, il est discuté de savoir si en utilisant le Cloud, l'avocat viole son obligation de préserver le secret professionnel. La réponse sera différente selon que l'on considère que le Cloud Provider est un auxiliaire ou non, puisque le professionnel peut, sauf instruction contraire, transmettre l'information à ses auxiliaires eux-mêmes astreints au secret professionnel dans la mesure nécessaire à la bonne exécution du mandat[46].

La *notion d'auxiliaire n'est toutefois pas définie* dans la loi, et ses contours sont relativement flous. Selon une première approche (extensive), sont considérées comme auxiliaires les personnes qui concourent à l'exécution du mandat du professionnel, ce qui inclut le secrétariat, dont la fonction est d'accompagner l'avocat dans chaque étape de son travail, mais exclut le personnel de nettoyage, dont la fonction n'est pas de traiter des informations confidentielles ni d'assister l'avocat dans l'exécution de sa mission[47]. Selon une deuxième approche (plus restrictive), l'auxiliaire doit fournir un soutien immédiat dans l'accomplissement des tâches du professionnel[48], ou encore être soumis à un rapport hiérarchique ou de subordination avec le professionnel[49]. Selon nous, la *question centrale est celle du lien fonctionnel,* soit de soutien au professionnel et de préservation de la confiance du public dans la profession. Le Cloud Provider mandaté pour gérer certaines prestations IT devrait être considéré comme un auxiliaire au sens de l'art. 321 CP vu le rôle significatif qu'il joue dans la préservation de la confiance du public dans la profession[50]. Il faut enfin souligner qu'il faudra aussi tenir compte de l'éventuelle volonté du client de limiter le cercle des auxiliaires, par exemple pour certaines transactions hautement confidentielles conduisant les avocats d'une même étude à signer des accords stricts de confidentialité (NDA). Il y a alors lieu de tenir compte de la volonté du client de ne pas divulguer d'information même à d'autres avocats d'une même étude et a fortiori à des auxiliaires, dont les prestataires IT.

2. Le consentement du client

Dans l'attente de règles ou de décisions claires quant à la qualification d'auxiliaire du Cloud Provider, l'approche prudente consiste à obtenir le consentement préalable du client. Le consentement n'est subordonné à aucune exigence de forme; il peut être exprès, tacite ou résulter d'actes concluants[51]. Il pourrait être objectivisé à la lumière d'une

42 Cette condition (indication des garanties appropriées et nom des pays vers lesquels les données sont transférées) ne ressort pas expressément de la LPD mais risque bien de s'imposer puisqu'elle pourrait ressortir d'une interprétation stricte de la LPD et de l'obligation d'un consentement éclairé et qu'elle est désormais prévue expressément dans le RGPD (art. 13 al. 1 let. f) et le P-LPD (art. 17 al. 4).

43 P. ex. la Circulaire FINMA 2018/3 Outsourcing précisant les conditions à l'externalisation en matière bancaire: l'ancienne version (2008/7) exigeait une information spécifique avec la possibilité de résilier la relation bancaire dans un délai de 30 jours en cas de transfert à l'étranger. La version actuelle ne prévoit plus de règles détaillées en matière de consentement du client mais suppose de se référer aux lois topiques (en particulier LB et LPD), dont le principe de précaution de la LB exige en principe aussi une information spécifique au client, respectivement un consentement exprès du client vu les exigences élevées en matière de secret bancaire et de confidentialité des données client.

44 *Supra* III 2.

45 Cf. CCBE, Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats, 7. 9. 2012, p. 6.

46 BERNARD CORBOZ, Les infractions en droit suisse, vol. 2, 3e éd. 2010, no 72 ad art. 321 CP.

47 CHAPPUIS/ALBERINI, (n. 4), p. 339.

48 WOLFGANG WOHLERS, (n. 6), p. 22.

49 NIKLAUS OBERHOLZER, in Basler Kommentar, Strafrecht II, Art. 111–392 StGB, 3e éd. 2013, no 10 ad art. 321 StGB.

50 Ce devrait être en tout cas le cas des prestations techniques et fonctionnelles de comptabilité, facturation et gestion des délais. Il pourrait être, en revanche, éventuellement discutable de savoir si la simple prestation d'hébergement des données joue aussi un tel rôle fonctionnel ou si au contraire elle devrait être exclue du rôle d'auxiliaire.

51 Cf. ATF 106 IV 133 c. 3, BERNARD CORBOZ, (n. 45), art. 321, N 48. Cf. WOLFGANG WOHLERS, (n. 6), indiquant que le consentement peut se faire par acte concluant mais doit être donné *«in eindeutiger und unmissverständlicher Art und Weise, so dass bei objektiver Betrachtung klar ist, in welche Handlungen der Geheimnisherr eingewilligt hat (und in welche nicht).»*

mise en balance des intérêts privés du client avec l'intérêt public d'une bonne administration de la justice.

L'avocat doit *en premier lieu défendre les intérêts de ses clients.* La défense de ces intérêts appelle au respect de la confidentialité relative aux affaires traitées, qu'elles soient d'ordre privé, commercial ou pénal. Qu'ils touchent au respect de la sphère privée, de la présomption d'innocence ou du maintien de la confidentialité d'informations commerciales, ces intérêts méritent tous autant d'être protégés. Ainsi et en premier lieu, la relation de confiance entre l'avocat et son client, comme la relation médecin-patient, ne peut se développer que si le client a la conviction que l'avocat mettra tout en œuvre pour le défendre au mieux; cette obligation découle des règles du mandat[52]. En deuxième lieu, la confiance découlera de *l'intérêt (économique) à une gestion efficiente* du dossier, laquelle requiert l'utilisation d'outils informatiques sûrs et performants. Enfin, la confiance découlera aussi du fait que *le client aura la conviction* que son défenseur garantit le maintien de toute la discrétion requise par l'affaire; ce besoin peut cependant varier d'un client à l'autre et d'un dossier à l'autre. Le maintien du secret ne vise cependant pas à protéger un hypothétique intérêt privé de l'avocat, qui découlerait du type d'activité déployé ou, comme l'exprime CHAPPUIS, *«pour s'abriter de reproches qui lui seraient adressés dans l'exercice de son mandat»*[53]. Alors que le principe sera celui du maintien du secret professionnel, l'avocat peut en être délié par son client[54]. En *troisième lieu,* la profession d'avocat doit *également être exercée dans le respect de l'intérêt public* d'une bonne administration de la justice, respectant les principes démocratiques, la liberté personnelle et la sphère privée (art. 31 al. 2 Cst., 6 par. 3 et 8 CEDH). En tant qu'auxiliaire de la justice, l'avocat contribue à ce que ces principes soient préservés. Le maintien du secret professionnel ne constitue ainsi pas un but en soi, mais un instrument parmi d'autres (notamment la séparation des pouvoirs) visant à une bonne administration de la justice. Le fait que la violation du secret professionnel soit poursuivie pénalement souligne l'importance de ce dernier dans ce contexte. Le fait qu'une telle violation ne soit pas poursuivie d'office, mais uniquement sur plainte relativise toutefois quelque peu son importance, le faisant dépendre de l'importance que lui confère le client en question dans un dossier particulier.

3. L'expression du consentement

C'est sur la notion de consentement que l'on pourra peu à peu se montrer progressiste. En effet, le temps avançant, la clientèle s'attendra de plus en plus à ce que de tels services soient utilisés – et peut-être même s'étonnera quand tel ne sera pas le cas; pour les cabinets de petite taille, le recours au Cloud peut même s'avérer nécessaire. D'aucuns estiment par ailleurs que la qualité d'auxiliaire justifie, sur le plan pénal, la divulgation d'informations secrètes entre le professionnel soumis à titre principal au secret professionnel et ses auxiliaires, pour autant que ces derniers apportent leur concours à la bonne exécution du mandat[55]. La communication de données couvertes par le secret professionnel à des tiers doit nécessairement reposer sur un motif justificatif. L'art. 321 ch. 2 et 3 CP autorise la divulgation d'informations couvertes par le secret professionnel dans trois cas spécifiques: les cas où la loi prévoit une obligation de renseigner une autorité ou de témoigner en justice, la levée du secret par l'autorité cantonale compétente et le consentement du maître du secret. Il faut ajouter à ces cas les motifs justificatifs généraux du CP, en particulier l'état de nécessité (art. 17 CP). Sans base légale idoine[56] et face à l'impossibilité pratique de requérir la levée du secret auprès de l'autorité cantonale compétente lors de chaque communication à un fournisseur Cloud, le consentement du client revêt une importance primordiale dans l'hypothèse où le prestataire Cloud n'est pas considéré comme un auxiliaire[57].

Le consentement prévu par l'art. 321 ch. 2 CP n'est soumis à aucune exigence de forme[58]. Il peut intervenir de manière expresse, par écrit ou par oral. Il peut également être donné tacitement ou par actes concluants[59], mais en principe pas de manière présumée ou hypothétique[60]. Les conditions posées par la doctrine pour le consentement tacite ou par actes concluants exigent que le client doit avoir connaissance du fait que les données vont être communiquées à l'extérieur de l'étude, sans quoi le consentement tacite ou par actes concluants sera difficile à admettre; l'autorisation ne doit pas être générale, une fois pour toutes[61]. La doctrine veut éviter qu'on prenne le consentement trop à la légère.

Dans la perspective d'une externalisation de données par recours à un Cloud, l'avocat serait bien inspiré de mentionner cette pratique dans le contrat de mandat, respecti-

52 BENOÎT CHAPPUIS, (n. 7), p. 53.
53 *Idem,* p. 166.
54 *Idem,* p. 164.
55 Par exemple: NIKLAUS OBERHOLZER, (n. 48), nº 20 ad art. 321 StGB; CHAPPUIS/ALBERINI, (n. 4), p. 339 ss.
56 Pour rappel, les conditions posées par les réglementations sur la protection des données ne permettent pas de justifier la divulgation d'une information couverte par le secret professionnel.
57 WOLFGANG WOHLERS, (n. 6), p. 59.
58 BERNARD CORBOZ, (n. 45), nº 48 ad art. 321 CP.
59 ATF 98 IV 217 c. 2; MICHEL DUPUIS ET AL. (édit.), Petit Commentaire Code pénal, 2012, nº 42 ad art. 321 CP.
60 La notion de consentement hypothétique est importée du droit médical et suppose pour le médecin d'établir que le patient aurait consenti au même s'il avait été dûment informé en tenant compte de la situation concrète et personnelle du patient (et non sur la base d'un «patient raisonnable»). Selon MEIER, cette notion est applicable aussi en matière de protection des données. Pour une approche restrictive du consentement hypothétique, arrêt du TAF A-3144/2008 du 27. 5. 2009, c. 12.1. MEIER rappelle que certains auteurs n'admettent le consentement hypothétique que lorsque le consentement ne peut objectivement pas être demandé, pas lorsqu'il a été simplement omis, mais que ces limitations ne se justifient guère puisqu'un consentement pourra être présumé ou l'intérêt privé prépondérant du patient justifiera le traitement. Le consentement hypothétique ne sera alors plus nécessaire. PHILIPPE MEIER, (n. 35), N 872.
61 PELET/SCHLOSSER, TARMED et le secret médical, in L'avocat et le juge face au droit pénal, Mélanges offerts à Eric Stoudman, 2005, p. 207; JÜRG BOLL, Die Entbindung vom Arzt- und Anwaltsgeheimnis, 1983, p. 42.

vement dans la procuration qui règle les relations internes avec le client. En ce sens, Wolfgang STRAUB propose la clause suivante: *«L'avocat peut externaliser la maintenance ou l'exploitation de ses systèmes informatiques. Par la signature du présent contrat, le client donne son accord à une éventuelle externalisation des données. L'avocat doit, quant à lui, s'assurer que toutes ses obligations professionnelles et la protection des données sont respectées en permanence. Lorsque des tiers et leurs collaborateurs engagés dans une externalisation sont susceptibles d'accéder aux données du client, ils doivent préalablement s'engager auprès de l'avocat à en garder le secret en tout temps.»*[62]

En l'absence de clause écrite ou de déclaration expresse du client, la licéité de la communication d'informations couvertes par le secret professionnel au prestataire Cloud dépend de l'existence ou non d'un consentement, qu'il intervienne de manière tacite ou par actes concluants. L'existence d'un tel consentement devrait être reconnue si le client peut raisonnablement s'attendre à ce que l'avocat recoure à un service Cloud pour la gestion de ses dossiers[63]. Cela sera de plus en plus le cas à l'avenir.

V. Conclusion

Sous l'angle du devoir de diligence contractuel et professionnel, l'avocat doit se doter d'une infrastructure informatique permettant d'assurer la sécurité des données. La question est de savoir quel avocat est le plus diligent: celui qui utilise le Cloud de manière précautionneuse ou celui qui y renonce. À notre sens, la solution Cloud pourrait s'imposer progressivement lorsque l'avocat n'est pas en mesure de se doter d'une infrastructure *in house* suffisamment sécurisée.

Aujourd'hui, la majorité des études d'avocats utilisent des systèmes informatiques (postes informatiques, laptops, serveurs, appareils mobiles, infrastructures réseau, softwares ou encore internet)[64]. Cela dit, toutes les études ne disposent pas, respectivement ne recourent pas aux mêmes moyens informatiques. Ceux-ci dépendent dans une double mesure de la stratégie informatique adoptée et des moyens financiers à disposition de l'étude[65]. Le choix d'une stratégie informatique particulière devrait reposer sur plusieurs critères, en particulier l'état des installations existantes, les besoins (ceux des clients, mais aussi ceux liés au fonctionnement de l'étude) ou l'évaluation des risques[66]. Quant au budget alloué à l'informatique, il dépend généralement du type et de la taille de l'étude. Depuis la popularisation des solutions Cloud publiques ou privées, les petites études ont dorénavant accès à des prestations informatiques encore inaccessibles il y a quelques années. Pour autant qu'elles soient correctement développées, l'externalisation des données par le biais d'un Cloud externe permettrait une gestion des données plus sécuritaire. Il existe donc un intérêt à ce que les avocats se rassemblent, notamment par le biais de fédérations ou d'associations, pour concentrer leurs efforts et obtenir des offres de services performantes. Ces efforts concertés réduiraient non seulement les coûts, mais ils permettraient surtout d'exercer une plus grande pression sur les fournisseurs de Clouds en vue d'obtenir des conditions d'utilisation conformes à l'exercice de la profession.

Sous l'angle de la protection des données, l'avocat devrait privilégier des systèmes ne donnant pas accès au contenu des données (p. ex. cryptage ou pseudonymisation des données avant le transfert des données sur les serveurs du Cloud Provider). Si le Cloud Provider a accès au contenu des données, l'utilisation du Cloud sera possible aux conditions de l'art. 10*a* LPD (en particulier contrat écrit, et traitements que le mandant serait en droit d'effectuer lui-même). En l'absence de dispositions légales ou règles professionnelles précises, nous ne voyons par ailleurs pas d'obstacle à recourir à un Cloud Provider établi à l'étranger[67], pour autant que les règles LPD en matière de transfert à l'étranger soient respectées (pays à niveau de protection adéquat ou moyennant des garanties contractuelles). Toutefois, vu la nature confidentielle des données et les exigences élevées en matière de consentement, il sera prudent de requérir le consentement exprès du client via l'insertion d'informations détaillées dans les conditions générales et/ou la lettre d'engagement, et de privilégier des Cloud Providers établis en Suisse, pour éviter le «risque pays».

Sous l'angle pénal enfin, la question se pose de savoir si en utilisant le Cloud, l'avocat viole son obligation de préserver le secret professionnel. La réponse sera différente selon que l'on considère que le fournisseur de services en nuage est un auxiliaire ou non et selon les tâches qui lui sont confiées (stockage des dossiers clients, comptabilité, facturation). Selon nous, et en ligne avec d'autres auteurs, le Cloud Provider doit être considéré comme un auxiliaire. À supposer que la conception inverse soit retenue (Cloud Provider comme tiers, non comme auxiliaire), ce sera finalement le client qui décidera du recours au Cloud. Une information claire sur la manière de travailler de l'étude et en particulier sur la manière dont les données sont sauvegardées sera nécessaire. Elle peut même constituer un critère permettant aux clients potentiels de choisir leur conseiller juridique ou leur avocat.

---

62 WOLFGANG STRAUB, Convention de mandat et informatique. Quels sont les points à régler?, Revue de l'Avocat 3/2013, p. 129, 130 ss.

63 En ce qui concerne les modalités du consentement d'anciens clients, éventuellement décédés, à l'externalisation des données après la fin du mandat, la question reste pour l'heure ouverte. WOLFGANG WOHLERS, (n. 14), p. 61, admet qu'il est exceptionnellement possible de recourir au consentement hypothétique du client lorsqu'il est impossible d'obtenir le consentement. Selon lui, les cas d'impossibilité se limiteraient aux cas où la personne est décédée et ne peut plus être questionnée. Le seul fait qu'il soit compliqué de contacter la personne concernée ne suffirait pas. Une autre solution parfois évoquée en doctrine consiste à maintenir un entreposage différencié entre les anciens dossiers et les dossiers pour lesquels un consentement à l'externalisation peut être admis.

64 WOLFGANG STRAUB, (n. 14), p. 516.

65 *Idem.*

66 *Idem.*

67 Rappelons que cette problématique existe déjà lorsque l'avocat utilise des services de *legal tech,* voire consulte ses e-mails depuis l'étranger et que cette distinction entre prestataires suisses et étrangers devient de plus en plus artificielle en cas de prestataire partie à un groupe étranger dont la société mère sise à l'étranger a un pouvoir de fait sur toutes les données du groupe, cf. 2.c).